Indonesian Journal of Mathematics Education
Vol. 2, No. 2, October 2019, pp: 69~74
p-ISSN: 2654-3907, e-ISSN: 2654-346X, DOI: 10.31002/ijome.v2i2.1813
e-mail: ijome@untidar.ac.id, website: jurnal.untidar.ac.id/index.php/ijome

Public Key Cryptosystem Based on Polynomial Composition

Maxrizal[1a)], Baiq Desy Aniska Prayanti[2b)]
[1]STMIK Atma Luhur, Jl. Jend. Sudirman Selindung, Pangkalpinang, Indonesia
[2]Universitas Bangka Belitung, Gg. IV No.1 Balun Ijuk, Merawang, Indonesia
e-mail: [a)]maxrizal@atmaluhur.ac.id, [b)]baiqdesyaniska@gmail.com

Received: 17th September 2019 *Revised: 26th October 2019* *Accepted: 30th October 2019*

Abstract

The public key cryptosystem is an extension of an asymmetric key cryptosystem. The public key cryptosystems have been developed based on the concepts of matrix, polynomial and polynomial decomposition. In this study, we will introduce the public key cryptosystem over polynomial composition. This research is a literature study. The results show that the polynomial composition can be used in public-key cryptosystems by modifying special functions to apply commutative properties.

Keywords: polynomial composition, the public key cryptosystem, polynomial key.

INTRODUCTION

The cryptosystem consists of a symmetry key cryptosystem and an asymmetric key cryptosystem. In symmetric-key cryptosystems, the sender and recipient of the message have the same private key. They must protect the private key of the other party to keep the message safe. For this reason, the sender and recipient of the message will send a private key through a secure path. Whereas in the asymmetric key cryptosystem, the recipient and sender of the message have different keys. In asymmetric key cryptosystems are known as private key and public key. A recipient of the message must generate the key pairs (public and private keys). Furthermore, the public key will be sent to the message sender. Next, the message sender will encrypt the plaintext (the original message). The results of encryption in the form of ciphertext. These results will be sent back to the recipient of the message. Furthermore, the recipient of the message will do a description to restore the plaintext (the original message) with the help of a private key.

In recent years, the symmetrical key cryptosystems are becoming obsolete. The asymmetric key cryptographic system is used and developed. The key pair of the asymmetric key cryptosystem is generated by the recipient of the message. Whereas in the latest developments the asymmetric key system is generated together by the sender and receiver of the message. This cryptosystem is known as the public-key cryptosystem. The public key cryptosystems have been developed on the non-commutative division semiring and matrix (Andrecut, 2015; Anjaneyulu & Sanyasirao, 2014; Dwivedi, et. al., 2011). Furthermore, the public key cryptosystems have also been developed for various matrix decomposition (Liu, et. al., 2016) and polynomial decomposition (Ezhilmaran & Muthukumaran, 2016; Tsaban, 2015; Valluri, 2014). Nevertheless, the developed public key cryptosystem still has weaknesses (Liu, et. al., 2017).

For this reason, in this paper, we will introduce a public-key cryptosystem developed on the concept of polynomial composition.

Basically, polynomial compositions are not commutative, so we will modify some polynomials so that they are commutative to the operation of polynomial compositions.

METHOD

This research is a literature study. The main reference in this study is a journal entitled Cryptanalysis of Schemes Based on Polynomial Symmetrical Decomposition. Furthermore, the proposed public key cryptosystem will be analyzed base on the function and polynomial composition (Anton & Rorres, 2013; Lang, 1993).

RESULTS AND DISCUSSION

Preliminaries

General linear group $GL_n\left(F_q\right)$ is a set of all $n\times n$-sized invertible matrices over finite fields. In mathematically, this concept is notated $GL_n\left(F_q\right)=\left\{a_{ij}\left|\det\neq 0\right.\right\}$. In this study, we choose $F_q=\mathbb{Z}_p$ so we get $GL_n\left(\mathbb{Z}_q\right)$. Since p is prime, the inverse element of nonzero elements is always present over modulo p. The number of elements (order of element) of $GL\left(n,\mathbb{Z}_p\right)$ is

$$\begin{aligned}\left|GL\left(n,F_q\right)\right| &= \left(q^n-1\right)\left(q^{n-1}-q\right)\ldots\left(q^n-q^{n-1}\right)\\ &= \prod_{k=0}^{n-1}\left(q^n-q^k\right)\end{aligned}.$$

If we have $GL\left(2,\mathbb{Z}_2\right)$, then the numbers of elements are $\left(2^2-1\right)\left(2^2-2\right)=6$, namely

$$GL\left(2,\mathbb{Z}_2\right)=\left\{\begin{bmatrix}1&0\\0&1\end{bmatrix},\begin{bmatrix}1&1\\1&0\end{bmatrix},\begin{bmatrix}1&1\\0&1\end{bmatrix},\begin{bmatrix}0&1\\1&1\end{bmatrix},\begin{bmatrix}1&0\\1&1\end{bmatrix},\begin{bmatrix}1&0\\0&1\end{bmatrix}\right\}.$$

Note that the determinants of the above matrices are not zero. If formed $A=\begin{bmatrix}1&2\\2&6\end{bmatrix}\in GL\left(2,\mathbb{Z}_7\right)$, then $\det\left(A\right)=2 \bmod 7=2$. Note that applies $2.4=8 \bmod 7=1$. Thus, we get

$$\begin{aligned}A^{-1} &= \frac{1}{\det\left(A\right)}\begin{bmatrix}d&-b\\-c&a\end{bmatrix}\\ &= 2^{-1}\begin{bmatrix}6&-2\\-2&1\end{bmatrix}\\ &= 4\begin{bmatrix}6&-2\\-2&1\end{bmatrix}\\ &= \begin{bmatrix}24&-8\\-8&4\end{bmatrix}\bmod 7\\ &= \begin{bmatrix}3&6\\6&4\end{bmatrix}\bmod 7\end{aligned}$$

Thus, an $A=\begin{bmatrix}1&2\\2&6\end{bmatrix}\in GL\left(2,\mathbb{Z}_7\right)$ always has an inverse of modulo p. Furthermore, $M_n\left(F_q\right)$ is a group with any size $n\times n$ matrix over the field F_q. Note that $GL_n\left(F_q\right)\subset M_n\left(F_q\right)$.

Description of Schemes Based on Polynomial Symmetrical Decomposition

The public key cryptosystem was introduced using the concept of Polynomial Symmetrical Decomposition (Liu, et. al., 2017). This scheme introduces the key generation between the sender and recipient of the message. This key agreement protocol uses a non-commutative group $\left(M_n\left(F_q\right),a,b\right)$, where $\left(M_n\left(F_q\right),.\right)$ is a non-commutative group and $a,b\in\mathbb{Z}$.

Suppose there is a polynomial $f\left(x\right)=4x^2+x+1\in F_5\left[x\right]$. We choose $P=\begin{bmatrix}1&2\\0&1\end{bmatrix}\in GL_2\left(F_5\right)$. Next, we form the polynomial symmetrical decomposition

$$f(P) = 4P^2 + P + I$$
$$= 4\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}^2 + \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$
$$= \begin{bmatrix} 6 & 18 \\ 0 & 6 \end{bmatrix} \bmod 5$$
$$= \begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix}$$

Next, we defined $f^a(P) = \underbrace{f(P)\ldots f(P)}_{a \text{ factor}}$.

Key Generator of Schemes Based on Polynomial Symmetrical Decomposition

We choose $P \in GL_n(F_q)$, $Q \in M_n(F_q)$, where $PQ \neq QP$. Output (P,Q) is a public key pair.

1. Max chooses any polynomial $f(x) \in F_q[x]$. He calculates $f(P) \in GL_n(F_q)$ and $y = f^a(P)Qf^b(P)$. He sends y to Baiq.
2. Baiq chooses any polynomial $h(x) \in F_q[x]$. She calculates $h(P) \in GL_n(F_q)$ and $u = h^a(P)Qh^b(P)$. He sends u to Max.
3. After the protocol running, Max and Baiq have the same key, i.e. $K = f^a(P)uf^b(P) = h^a(P)yh^b(P)$.

   This is proven as follows

$$f^a(P)uf^b(P)$$
$$= f^a(P)\left[h^a(P)Qh^b(P)\right]f^b(P)$$
$$= \left[f^a(P)h^a(P)\right]Q\left[h^b(P)f^b(P)\right]$$
$$= \left[h^a(P)f^a(P)\right]Q\left[f^b(P)h^b(P)\right]$$
$$= h^a(P)\left[f^a(P)Qf^b(P)\right]h^b(P)$$
$$= h^a(P)yh^b(P)$$

Furthermore, encryption and description lie in the agreement of the sender and receiver. In this study, we use the addition operation and the inverse of adding integers. If there is a message (plaintext) P then encryption $C = P + K$. Next, to get P, we do the description $P = C - K$.

In essence, this scheme offers the use of a matrix and its decomposition to build key generation protocols.

Description of Schemes Based on Polynomial Composition

In the proposed scheme, we designed a simpler key generation system. We don't have to use matrix computation and its complex decomposition. This public key cryptosystem was developed based on the concept of polynomial composition. If any polynomials $g(x) \in F_q[x]$ and $j(x) \in F_q[x]$ are given then $(g \circ j)(x) \neq (j \circ g)(x)$ does not apply. Next, we choose $f(x) = ax$ and $h(x) = bx$, with $a,b \in \mathbb{Z}$. Note that applies

$$(f \circ h)(x) = f(h(x))$$
$$= f(bx)$$
$$= abx$$
$$= bax$$
$$= h(ax)$$
$$= h(f(x))$$
$$= (h \circ f)(x)$$

Thus, we get $(f \circ h)(x) = (h \circ f)(x)$, where $f(x) = ax$ and $h(x) = bx$, with $a,b \in \mathbb{Z}$.

Suppose there is a polynomial $g(x) = 4x^2 + x + 1 \in F_5[x]$. We choose $f(x) = 2x \in F_5[x]$ and $h(x) = 4x \in F_5[x]$. Next, we form

$$(f \circ g)(x) = f(g(x))$$
$$= (8x^2 + 2x + 2) \bmod 5$$
$$= 3x^2 + 2x + 2$$

and

$$\begin{aligned}(g\circ f)(x) &= g(f(x))\\ &= (16x^2+2x+1)\bmod 5\\ &= x^2+2x+1.\end{aligned}$$

Note that $(f\circ g)(x)\neq(g\circ f)(x)$ and $(h\circ g)(x)\neq(g\circ h)(x)$. Nevertheless, we have $(f\circ h)(x)=(h\circ f)(x)$. We will apply these special characteristics to the proposed algorithm.

Key Generator of Schemes Based on Polynomial Composition

We choose any polynomial $g(x)\in F_q[x]$. Output $g(x)$ is a public key.

1. Max chooses any polynomial $f(x)=ax$. He calculates $y(x)=(f\circ g\circ f)(x)$ and sends $y(x)$ to Baiq.
2. Baiq chooses any polynomial $h(x)=bx$. She calculates $u(x)=(h\circ g\circ h)(x)$ and sends $u(x)$ to Max.
3. After the protocol running, Max and Baiq have the same key, i.e. $K(x)=(f\circ u\circ f)(x)=(h\circ y\circ h)(x)$. This is proven as follows

$$\begin{aligned}(f\circ u\circ f)(x) &= (f\circ(h\circ g\circ h)\circ f)(x)\\ &= ((f\circ h)\circ g\circ(h\circ f))(x)\\ &= ((h\circ f)\circ g\circ(f\circ h))(x)\\ &= (h\circ(f\circ g\circ f)\circ h)(x)\\ &= (h\circ y\circ h)(x)\end{aligned}$$

Furthermore, encryption and description lie in the agreement of the sender and receiver. In this study, we use encryption and description with function value operations.

If there is a message (plaintext) P then encryption and description use the function $C=K(P)$. So, we use the inverse principle of the function in the description.

Simulation of Schemes Based on Polynomial Composition

Max and Baiq will send a message. They will generate the key. Max and Baiq agreed to use $g(x)=4x+5\in F_7[x]$. Suppose they choose a polynomial over field F_7 .

1. Max chooses any $f(x)=2x$ and counts

$$\begin{aligned}y(x) &= (f\circ g\circ f)(x)\\ &= f(g(f(x)))\\ &= f(g(2x))\\ &= f(8x+5)\\ &= (16x+10)\bmod 7\\ &= 2x+3.\end{aligned}$$

   Max sent $y(x)=2x+3$ to Baiq.
2. Baiq chooses any $h(x)=3x$ and counts

$$\begin{aligned}u(x) &= (h\circ g\circ h)(x)\\ &= h(g(h(x)))\\ &= h(g(3x))\\ &= h(12x+5)\\ &= (36x+15)\bmod 7\\ &= x+1.\end{aligned}$$

   Baiq sent $u(x)=x+1$ to Max.
3. After the protocol running, Max forms a key

$$\begin{aligned} K &= (f \circ u \circ f)(x) \\ &= f\left(u\left(f(x)\right)\right) \\ &= f\left(u(2x)\right) \\ &= f(2x+1) \\ &= 4x+2 \end{aligned}$$

and Baiq forms a key

$$\begin{aligned} K &= (h \circ y \circ h)(x) \\ &= h\left(y\left(h(x)\right)\right) \\ &= h\left(y(3x)\right) \\ &= h(6x+3) \\ &= (18x+9) \bmod 7 \\ &= 4x+2. \end{aligned}$$

Note that the key on Max is the same as the Baiq key.

Encryption:

Max has the message "YANKA". In this case, Max and Baiq agreed to use a letter conversion table.

Table 1. Letter Conversion Table

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**
1	2	3	4	5	6	7	8
I	**J**	**K**	**L**	**M**	**N**	**O**	**P**
9	10	11	12	13	14	15	16
Q	**R**	**S**	**T**	**U**	**V**	**W**	**X**
17	18	19	20	21	22	23	24
Y	**Z**						
25	0						

The message "YANKA" becomes "25-1-14-11-1". Next, Max does the calculation with $K = 4x+2$ and he has

$$\begin{aligned} C_1 &= K(P_1) \\ &= K(25) \\ &= 4(25)+2 \\ &= 102 \\ C_2 &= K(P_2) \\ &= K(1) \\ &= 4(1)+2 \\ &= 6 \\ &\vdots \\ C_5 &= K(P_5) \\ &= K(1) \\ &= 4(1)+2 \\ &= 6 \end{aligned}$$

So, Max gets

P_i	C_i
25	102
1	6
14	58
11	46
1	6

Furthermore, Max sent “102-6-58-46-6” to Baiq.

Description:

Baiq received “102-6-58-46-6” from Max. Baiq also has an key $K = 4x+2$. If there is C_i then

$$\begin{aligned} C_i &= K(P_i) \\ C_i &= 4P_i + 2 \\ P_i &= \frac{C_i - 2}{4} \end{aligned}$$

Thus, Baiq obtained

$$P_1 = \frac{C_1 - 2}{4}$$
$$= \frac{102 - 2}{4}$$
$$= 25$$
$$P_2 = \frac{C_2 - 2}{4}$$
$$= \frac{6 - 2}{4}$$
$$= 1$$
$$\vdots$$
$$P_5 = \frac{C_5 - 2}{4}$$
$$= \frac{6 - 2}{4}$$
$$= 1$$

So, Baiq gets

C_i	P_i
102	25
6	1
58	14
46	11
6	1

Baiq obtained "25-1-14-11-1". He gets the message "YANKA" with the help of the letter conversion table.

CONCLUSION

The concept of polynomial composition can be applied to public-key cryptosystems by giving special conditions in the form of functions $f(x) = ax$ and $h(x) = bx$. Based on these characteristics, we can form a key agreement protocol so that the public key cryptosystem can run well.

REFERENCES

Andrecut, M. (2015). *A matrix public key cryptosystem*, 1–18.

Anjaneyulu, G. S. G. N., & Sanyasirao, A. (2014). Distributed group key management protocol over non-commutative division semirings. *Indian Journal of Science and Technology*, *7*(6), 871–876.

Anton, H., & Rorres, C. (2013). *Elementary linear algebra: Applications version, 11th Edition*. Wiley eGrade.

Dwivedi, A., Ojha, D. B., Sharma, A., & Mishra, A. (2011). A model of key agreement protocol using polynomials over non-commutative division semirings. *Journal of Global Research in Computer Science*, *2*(3), 40–43.

Ezhilmaran, D., & Muthukumaran, V. (2016). Key exchange protocol using decomposition problem in near ring. *Gazi University Journal of Science*, *29*(1), 123–127.

Lang, S. (1993). *Linear algebra*. New York: Springer.

Liu, J., Zhang, H., & Jia, J. (2017). Cryptanalysis of schemes based on polynomial symmetrical decomposition. *Chinese Journal of Electronics*, *26*(6), 1139–1146. https://doi.org/10.1049/cje.2017.05.005

Liu, J., Zhang, H., Jia, J., Wang, H., Mao, S., & Wu, W. (2016). Cryptanalysis of an asymmetric cipher protocol using a matrix decomposition problem. *Science China. Information Sciences*, *59*(May), 1–11. https://doi.org/10.1007/s11432-015-5443-2

Tsaban, B. (2015). Polynomial-time solutions of computational problems in noncommutative-algebraic cryptography. *Journal of Cryptology*, *28*(3), 601–622. https://doi.org/10.1007/s00145-013-9170-9

Valluri, M. R. (2014). Zero-knowledge authentication schemes using quasi-polynomials over non-commutative groups. *Open Journal of Information Security And Applications*, *1*(1), 43–50.